IN REPLY
REFER TO: PL6

8 Mar 2005

1. DISA has a requirement for NCES Service Oriented Architecture (SOA) Framework Support. The period of performance is 10 months from date of award. The anticipated contract type is T&M.

2. It is requested that you submit a written technical and cost proposal in response to the attached performance based work statement. Please prepare the proposal in accordance with the terms and conditions of the NetCents contract. Your proposal or "no-bid reply" shall be submitted no later than **18 Mar 05 at 2:00 (CT).**

3. This is a best value award and the customer agency has indicated that Section 508 Accessibility Standards do not apply to this requirement. Therefore, the evaluation criteria for this award will be based on Past Performance, Technical/Management Approach and Other Factors. The selection criteria factors are listed in attachment 1.

4. Questions should be addressed to the Contracting Officer at the following e-mail address: Linda.Goff@disa.mil. Please provide any questions, in writing, no later than **14 Mar 2005, 12:00 (CT).** Questions received after this date may or may not be answered. My telephone number is (618) 229-9486 if you need to contact me.

Sincerely,

2 Enclosures a/s

LINDA K. GOFF
Contracting Officer

EVALUATION CRITERIA
for
NCES Service Oriented Architecture (SOA) Framework Support

A. <u>GENERAL</u> **A board of qualified personnel shall evaluate each proposal submitted to this Statement of Work (SOW). Judgment on the part of the government is implicit in the entire process.**

The evaluation of technical features includes an assessment to determine if the proposed solution satisfies the government's objectives and provides for high quality performance. The three evaluation factors described below will be used to evaluate vendor proposals. The assessment will address the following factors, listed in descending order of importance:

Factor 1 - Past Performance
Factor 2 - Technical Solution
Factor 3 - Cost/Price

The factors shown above are listed in their order of importance. Factor 1, Past Performance and Factor 2, Technical Solution, are significantly more important than Factor 3 Cost. Factor 1, Past Performance is more important than Factor 2, Technical Solution. However, Cost/Price will become increasingly important as evaluation ratings for Past Performance and Solution Factors approach equal.

Color Ratings. A color rating depicts how well the offeror's proposal meets the evaluation standards and SOW requirements. The Past Performance and Technical Solution areas will receive color ratings, Cost/Price will not. Proposals will be rated on the basis of the following color code and risk system:

Factor 1:

Color	Past Performance
Blue	Highly relevant/very recent past performance in all identified past performance efforts; excellent performance ratings.
Green	Relevant/somewhat recent past performance in all identified past performance efforts; acceptable performance ratings.
Yellow	Somewhat relevant/not very recent past performance; mostly acceptable performance ratings.
Red	Little relevant past performance identified; almost all unacceptable performance ratings.
White	Completely lacks relevant performance history or is unavailable.

Factor 2:

COLOR	RATING	DEFINITION

BLUE	Exceptional	The vendor's proposal offers approaches/solutions that when implemented, are expected to result in superior achievement of DISA objectives with minimal risk. A "Blue" rating indicates that the proposal contains significant strengths and few or no weaknesses.
GREEN	Acceptable	The vendor's proposal offers approaches/solutions that if implemented, introduce moderate risk but are considered likely to produce performance results meeting DISA objectives. A "Green" rating indicates that the proposed solution contains a number of strengths, but also some weaknesses.
YELLOW	Marginal	The vendor's proposal offers approaches/solutions that if implemented, introduce a high risk that expected performance would achieve DISA objectives. A "Yellow" rating indicates that the proposed solution contains strengths, but also significant weaknesses.
RED	Unacceptable	The vendor's proposal offers approaches/solutions that if implemented, would introduce excessive risk making it highly unlikely that performance would meet DISA objectives. A "Red" rating indicates that the proposed solution, while maybe presenting some strengths, also contains significant weaknesses.

Past Performance

Contractor shall describe all relevant contracts completed within the past three years and on current contracts performed by the contractor or its subcontractors performing any technical tasks related to this SOW. Specifically, contractor current or completed contracts must demonstrate mastery of and experience in the areas of Service Oriented Architectures (SOA), especially in the areas of Service Discovery, Security Services and Enterprise Service Management. Contractor shall describe clearly that the contractor has competently performed work of the size, scope, and complexity as required by the SOW. This experience must include demonstrated performance in the development and refinement of architectures, engineered solutions based on these architectures, and reference implementations of the engineered solutions. Past performance should also show knowledge of and participation in pilots and demonstrations based on reference implementations. Contractor must demonstrate a competent knowledge of the NCES program. Contractor must demonstrate expertise in contractor/contractor and contractor/government partnering or team environments and the ability to work cooperatively with other contractors to ensure that the government's piloting and demonstration goals are met.

Technical Approach

Technical: Contractor shall describe knowledge in the areas of full life cycle software engineering, analytical activities and architecture development in SOAs, development of engineering solutions, deployment of engineered solutions in reference implementations, and use of reference implementations for enterprise piloting and demonstration activities. Contractor must demonstrate a clear understanding of the government requirements. Contractor must demonstrate knowledge and expertise in the three areas of Service Discovery, SOA Security, and Enterprise Service Management. Contractor must be knowledgeable with Web Service

Registries, replication of these registries, SOA governance, and technical approaches to managing Web Services.

Management: Contractor shall describe an acceptable approach for assessing project status and assuring timely government cognizance of project progress.

Cost realism. Labor categories and proposed staffing levels are appropriate, sufficient to accomplish the required work.

Proposed staffing (experience, education, skills) is appropriate to job function and proposed labor category/title. Contractor shall describe by name key personnel- dedicated management and technical individuals - with the technical skills, education, employment, commitment, and experience adequate to accomplish the SOW tasks. Resumes of key personnel will document experience and/or education in software development life cycle, SOAs, software/system/network engineering, enterprise computing, and web services development and deployment.

Cost / Price

This factor will evaluate the price proposal offered by the company. The intent of the evaluation is to determine whether the proposed cost/price elements are realistic for the work to be performed, reflect a clear understanding of the requirements, and are consistent with the approach described in the vendor's technical proposal.

The proposed prices will be evaluated with respect to their completeness and reasonableness. The reasonableness of the overall price will be determined by adequate price competition. The proposed prices may also be compared to the Independent Government Cost Estimate (IGCE).

Award Criteria

a. The following conditions must be met in order to be eligible for award:

1. The proposal must comply in all material respects with the requirement of the law, regulation and conditions set forth in the SOW.

2. The proposal must meet all mandatory SOW requirements.

3. The offeror must be determined responsible according to the standards of FAR Part 9, Subpart 1.

b. Best Value Determination - Upon satisfaction of the above conditions, the government will select the offeror whose proposal reflects the best combination of past performance, technical solution, and cost/price. A time-and-material contract will be awarded by source selection procedures to the offeror whose proposal reflects the overall best value to the government. The Government reserves the right to award to an offeror with other than the lowest price offer, or other than the highest technically rated offer.

c. Award all or none basis – The government intends to award one to the vendor whose proposal is identified as offering the best value solution. The government intends to award a single contract but reserves the right to award multiple contracts as a result of this competition.

d. The government reserves the right to not award a contract as a result of this competition, if in the opinion of the Contracting Officer, none of the submitted proposals would provide satisfactory performance.

STATEMENT OF WORK

NCES Service Oriented Architecture Framework Support

As of 24 Feb 2005

1. **Points of Contact**

a. TM   Lee Jarrell, DISA/NE31
          5275 Leesburg Pike
          Falls Church, VA 22041
          703-882-1771
          emmett.jarrell@disa.mil

b. Alternate TM   Hung Truong, DISA/NE31
          5275 Leesburg Pike
          Falls Church, VA 22041
          703-882-1519
          hung.truong@disa.mil

2. **Task Order Title: NCES Service Oriented Architecture (SOA) Framework Support**

3. **Background.**

DISA is required by the DOD to enhance communications effectiveness through improved information interoperability. The Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) has articulated a vision for transforming the information environment in the DOD. This vision calls for a move from the centralized thinking and planning currently reflected in the Task, Process, Exploit, Disseminate (TPED) paradigm, to an edge-centered Task, Post, Process, Use (TPPU) approach to information sharing and availability. The envisioned changes represent a fundamental paradigm shift from providing platform centric applications to platform independent, web-enabled, Net-Centric services requiring the support of a ubiquitous network environment, richly populated with information of value, as determined by the consumer, which is highly available, secure, and reliable.

The Global Information Grid (GIG) Enterprise Services (GES) will provide visibility and access to data, enabling the end user to execute an intelligent pull of mission-tailored information from anywhere within the network environment and at anytime. In addition to directly supporting the information processing needs of edge and GIG users, the NCES program will architect and field a set of network-accessible foundational capabilities, known as Net-Centric Enterprise Services. These services will be standards-based, and will provide a common infrastructure that facilitates the construction and deployment of enterprise applications and services.

The NCES foundational components are based upon a Service Oriented Architecture, or "SOA". This type of architecture provides a scalable, robust, highly available network of interoperable services that can be dynamically consumed and assembled in real-time. In essence, the NCES SOA is a framework for providing data sources and applications to the GIG, and making them discoverable and consumable within and across Communities of interest.

4. Objective.

The objective of this Statement of Work (SOW) is to specify the planning, management, coordination and technical support services related to and necessary for the pilot fielding of the Service Discovery, Security, and Enterprise Service Management services in support of achieving Milestone B approval for the NCES program.

5. Scope.

The scope of work for the tasks described herein includes support for planning, design, development and, pilot fielding of the Service Discovery, Security, and Enterprise Service Management services. Limited sustainment support will also be provided through bug fix and maintenance releases of the services.

6. Specific Tasks

The contractor shall perform the following tasks related to overall management of this effort.

6.1. Task 1. Task Order Management

The contractor shall provide the technical and functional activities as required by the government for integration of all tasks specified within this Statement of Work to include productivity and management methods such as Quality Assurance, Progress/status reporting, and Program Reviews.

The contractor shall provide administrative and clerical support for documentation, briefings, and functions related to managing the task order set forth in this statement of work.

The contractor shall provide a draft Work Breakdown Schedule (WBS) illustrative of the tasks to be monitored, and prepare a task order management plan describing the technical approach, organizational resources and management controls to be employed to meet the cost, performance and schedule requirements throughout task order execution.

The contractor shall provide quarterly In-Progress Reviews and Monthly Status Reports describing task progress, accomplishments, financial status, and problems. At a minimum, this data shall include:

> The project schedule showing any proposed changes, the reasons for changes, and the potential impact on the program.

> Descriptions of activities and deliverables during the current month for the task order. The descriptions shall include problem definitions and recommendations for program resolutions. Particular attention shall be given to risk management activities.

> Budget estimates (actual and revised) of overall and monthly projected staff-hours and resource costs for the task order; and estimates (actual and revised) of overall and monthly projected staff hours and costs by task

> Trips, technical visits, and related results for the reporting period.

> Identification of key personnel, personnel reassignments including all personnel added to or removed from the task order by task.

The monthly status report shall show cumulative planned hours, cumulative actual hours, cumulative Other Direct Costs (ODCs), and cumulative actual dollars by task and subtask; cumulative actual hours and cumulative actual labor cost by subtask; and staff hours by subtask for the reporting period. An explanation of any deviations of actual expenditures from planned costs, as indicated in the management plan shall be included in the Monthly Status Report.

For each task per major WBS element per month (i.e., Month 1, Month 2, Month 3...), the contractor shall provide the following schedule and cost data in tabular form:

- Estimate at Completion (EAC)
- Budget at Completion (BAC)
- Budgeted Cost of Work Scheduled (BCWS)
- Budgeted Cost of Work Performed (BCWP)
- Actual Cost of Work Performed (ACWP)

The WBS and related data shall be provided in a Microsoft Project compatible format.

6.2. Task 2. NCES Service Discovery

To ensure successful integration, all subtasks will be accomplished in strict accordance and compliance with technical guidance and software engineering processes established by the NCES Technical Integrator.

6.2.1. Architecture.

6.2.1.1. The contractor shall support the government in the continued definition and refinement of the NCES Service Discovery architecture. The contractor will be required to align the architecture with emerging discovery standards (e.g. UDDI 3.0, WS-Discovery, etc) and ensure that the architecture meets the evolutionary needs of the pilot communities (e.g. NCCP, Horizontal Fusion). The contractor will work with agencies, services, unified commands and other NCES contractors to solicit requirements and feedback to support the evolution of the architecture. The contractor will be required to produce incremental releases of architecture documentation including a System Architecture document and service specification. Focus areas for the next year will include, but not be limited to, federated service discovery, governance, tighter integration with Security, DDMS support, and enhanced COI/Enterprise taxonomies.

6.2.1.2. The contractor shall define an architecture and deployment strategy for NCES Service Discovery Services. The deployment strategy will consist of a rollout plan, and an analysis of the advantages and disadvantages for each deployment option. The architecture and strategy will address deployment on SIPRNET and NIPRNET, and will include alternatives for both enterprise and COI deployment. Functional alternatives for deployment such as "federated search" vs. "data replication" will be outlined and considered.

6.2.1.3. The contractor shall support the government in facilitating and participating in the Service Discovery Working Group. The contractor will be required to host the working group meetings and distribute meeting minutes and action lists.

6.2.1.4.   The contractor shall work to refine the Service Discovery CONOPS to incorporate lessons learned, community feedback, and future architecture direction. The contractor will be required to produce incremental releases of the document to support pilot integration and usage of the Service Discovery Services.

6.2.2.   Engineering.

6.2.2.1.   The contractor shall refine the NCES Service Discovery Services reference implementation to address emerging community requirements and future architecture direction, e.g., enterprise/COI federated implementation and integration of a governance capability. The development of the reference implementation will follow an agile, iterative software development process and the contractor will be required to provide software releases on a release schedule defined by the government.

6.2.2.2.   The contractor shall develop graphical application components that support the management of Service Discovery Services and provide key capabilities to end-users such as service publishing, service discovery, and management of service metadata including security policies. The application components will need to be integrated into existing portal solutions and be required to support industry standards (e.g. JSR-168 or WSRP).

6.2.2.3.   The contractor shall develop testing documentation to include test cases and test scenarios in electronic and automated formats. The contractor shall define all test related data sets and execute product testing cycles prior to release approval. The contractor will perform regression testing as required and maintain metrics on test coverage.

6.2.2.4.   The contractor shall support the government in the definition of formal new release scopes and the management of integration support requests. The contractor shall have formal participation at CCB meetings for review and approval of new release scopes and integration support activities.

6.2.2.5.   The contractor shall produce key engineering documents and artifacts including the following:

- Integration guide
- Requirements documentation including use cases, SRS, and RTM
- System architecture document
- Service specifications with annotated Web Services Description Language (WSDL) files
- User guides and tutorials
- Test plans, test scenarios and test suites
- Installation guides
- Developer/integrator guides

6.2.2.6.   The contractor shall engineer an SDK to support the rapid integration of the Service Discovery Services into the pilot applications. The SDK will be required to support both Java and .NET. The contractor shall provide robust documentation sets along with sample applications to support rapid integration and acceptance of the SDK.

6.2.3. Outreach and Integration.

6.2.3.1. The contractor shall provide hands-on support to the NCC Pilot program pilot. The contractor will be required to support the portfolio members in architecting their solutions to integrate into the Service Discovery Services architecture. The contractor will also be required to provide hands-on development and integration support to ensure the pilot programs can leverage the Service Discovery Services reference implementation. The contractor will also provide a log of all support activities assigned and completed, and trip and site visit status reports.

6.2.3.2. The contractor shall support program reviews and technical exchange meetings by both the NCES program and the community pilot programs (e.g. NCCP, Horizontal Fusion). The contractor will prepare briefings that communicate project status and technical details on the Service Discovery Services. On the average, one technical exchange meeting or equivalent is expected per week with one deliverable (briefing, report, etc.) per meeting.

6.2.3.3. The contractor shall prepare training materials for the Service Discovery service to include technical installation, administration and setup of the service as well as functional sample application exercises and use cases.

6.2.4. Technical Support.

6.2.4.1. The contractor shall provide maintenance releases of the Service Discovery Services reference implementation to address the change requests of the pilot community. The contractor will be required to work closely with government staff to prioritize requests and vet releases through the defined change control process as defined in the CCB charter.

6.2.4.2. The contractor shall support the deployment and fielding of Service Discovery Services to support pilot activities. The scope of the deployments will include instances of Service Discovery Services in the following environments: DISA DECC (SIPRNET), COI, and NIPRNET. The contractor will provide hands-on support for installation, deployment, and other hosting-related issues for Service Discovery. The contractor will also provide a log of all support activities assigned and completed and any trip and site visit status reports.

6.2.4.3. The contractor shall support the capture of CDD-defined metrics to support test and evaluation.

6.2.4.4. The contractor shall support the development of C&A documentation and application-level testing in support of the deployment of Service Discovery Services on NIPR/SIPRNET. The contractor will be required to support acceptance testing, vulnerability testing, etc. The contractor will also be required to develop key accreditation documentation artifacts including the SSAA and Appendix T documents.

6.3. Task 3. NCES Security Services

To ensure successful integration, all subtasks will be accomplished in strict accordance and compliance with technical guidance and software engineering processes established by the NCES Technical Integrator.

6.3.1. Architecture.

6.3.1.1.   The contractor shall support the government in the continued definition and refinement of the NCES Security Services architecture. The contractor will work with agencies, services, unified commands and other NCES contractors to solicit requirements and feedback to support the evolution of the architecture. The contractor will be required to produce incremental releases of architecture documentation including a System Architecture document.

6.3.1.2.   The contractor shall support the government in the definition of the enterprise deployment architecture for the NCES Security Services. The contractor will be responsible for weighing several alternatives including centralized/replicated and decentralized/federated and prepare formal assessments to determine the optimal approach.

6.3.1.3.   The contractor shall support the government in facilitating/participating in community working group meetings focused on NCES Security Services architecture and fielding topics. The contractor will be required to host the working group meetings and distribute meeting minutes and action lists.

6.3.1.4.   The contractor will work with other DoD working groups and organizations, and will align the Security Services architecture with IA Component of the GIG SPO requirements and other emerging DoD requirements.

6.3.1.5.   The contractor will perform an industry analysis of COTS tools to determine the alignment and integration impact with the Security Services architecture. The contractor will combine the findings into a living document that details the key architectural components of the Security Services solution, provides a gap analysis between the products provided by the current market and the Security Services architecture, and includes an objective market study of emerging technologies and the maturation of those components.

6.3.1.6.   The contractor will create a Security Services specification document that details an abstraction layer sufficient to provide Security Services to the enterprise while maintaining vendor- and product- independence. The specification document will contain marked up Web Service Description Language (WSDL) documents, usage scenarios, a documented set of APIs, a detailed set of processing rules, and other data necessary to detail the business rules provided by the Security Services. The specification document can be used as a guidebook when integrating either COTS or GOTS software as components that back the Security Services implementation.

6.3.2. Engineering.

6.3.2.1.   The contractor shall refine the NCES Security Services reference implementation to address emerging community requirements and future architecture direction. The

development of the reference implementation will need to follow an agile, iterative software development process and the contractor will be required to provide software releases on a schedule defined by the government. The reference implementation will also be aligned with the Security Services specification and architecture documents.

6.3.2.2. The contractor shall develop testing documentation to include test cases and test scenarios in electronic and automated formats. The contractor shall define all test related data sets and execute product-testing cycles prior to release approval. The contractor will perform regression testing as required and maintain metrics on test coverage.

6.3.2.3. The contractor shall support the government in the definition of formal new release scope and the management of integration support requests. The contractor shall have formal participation at CCB meetings for review and approval of new release scope and integration support activities.

6.3.2.4. The contractor shall perform work to integrate commercial security solutions (e.g. XML firewall, policy management) into the Security Services architecture to vet architecture, accelerate time-to-market and demonstrate value of specification-based approach.

6.3.2.5. The contractor shall produce key engineering documents and artifacts including the following:

- Integration guide
- Requirements documentation including use cases, Software Requirements Specification, and Requirements Tracability Matrix
- System architecture document
- Service specifications with annotated Web Services Description Language (WSDL) files
- User guides and tutorials
- Test plans, test scenarios and test suites
- Installation guides
- Developer/integrator guide

6.3.2.6. The contractor shall engineer an extensible SDK framework to support DISA integration and pilot partners on platforms not currently supported by the Security Services SDK. The SDK framework will provide "ground-start" libraries and capabilities that shorten the integration lifecycle by providing commonly used software components. A mechanism will be provided to allow SDK "plug-ins" to be built that enable the core capabilities to be used on a wide variety of platforms. The contractor will be responsible for formulating an approach to verify that new extensions integrated into the SDK framework can be validated and certified as SDK- and Security Services-compliant. The contractor shall provide robust documentation sets along with sample applications to support rapid integration and acceptance of the SDK.

6.3.2.7. The contractor shall engineer plug-in extensions to the SDK to support the platform requirements as defined by the NCES and pilot communities. Example platforms include WebLogic, Apache Axis, Systinet, GLUE, .NET, etc. In addition to the plug-

in functionality, detailed integration for the chosen platforms will be provided, that details step-by-step integration guidelines, a sample application, and expected results document.

6.3.3. Outreach and Integration.

6.3.3.1. The contractor shall provide hands-on support to the NCC Pilot program. The contractor will be required to support the portfolio members in architecting their solutions to integrate into the Security Services architecture. The contractor will also be required to provide hands-on development and integration support to ensure the pilot programs can leverage the Security Services reference implementation.

6.3.3.2. The contractor shall support program reviews and technical exchange meetings required by both the NCES program and community pilot programs (e.g. NCCP, Horizontal Fusion). The contractor will prepare briefings that communicate project status and technical details on the Security Services. On the average, one technical exchange meeting or equivalent is expected per week with one deliverable (briefing, report, etc.) per meeting.

6.3.3.3. The contractor shall deliver scheduled knowledge transfer sessions to DISA personnel.

6.3.4. Technical Support.

6.3.4.1. The contractor shall provide maintenance releases of the Security Services reference implementation to address the change requests of the pilot community. The contractor will be required to work closely with government staff to prioritize requests and vet releases through the defined change control process as defined in the CCB charter.

6.3.4.2. The contractor shall support the deployment and fielding of Security Services to support pilot activities. The scope of the deployments will include instances of Security Services in the following environments: DISA DECC (SIPRNET), COI, and NIPRNET. The contractor will provide hands-on support for installation, deployment, and other hosting-related issues for Security Service.

6.3.4.3. The contractor shall support the capture of CDD-defined metrics to support test and evaluation.

6.3.4.4. The contractor shall support the development of C&A documentation and application level testing to support the deployment of Security Services on NIPR/SIPRNET. The contractor will be required to support acceptance testing, vulnerability testing, etc. The contractor will also be required to develop key accreditation documentation artifacts including the SSAA and appendix T documents.

6.4. Task 4. NCES Enterprise Service Management (ESM)

To ensure successful integration, all subtasks will be accomplished in strict accordance and compliance with technical guidance and software engineering processes established by the NCES Technical Integrator.

6.4.1. Architecture

6.4.1.1.   The contractor shall support the government in the continued definition and refinement of the NCES ESM architecture. The contractor will work with agencies, services, unified commands and other NCES contractors to solicit requirements and feedback to support the evolution of the architecture. The contractor will be required to produce incremental releases of architecture documentation including a System Architecture document.

6.4.1.2.   The contractor shall support the government in the definition of the enterprise deployment architecture for the NCES ESM. The contractor will be responsible for weighing several alternatives including centralized/replicated and decentralized/federated and prepare formal assessments to determine the optimal approach.

6.4.1.3.   The contractor shall support the government in facilitating/participating in community working group meetings focused on NCES ESM architecture and fielding topics.

6.4.1.4.   The contractor will create an ESM specification document that details the capabilities provided by ESM to the enterprise while maintaining vendor- and product-independence. The specification document will contain marked up Web Service Description Language (WSDL) documents, usage scenarios, a documented set of APIs, a detailed set of processing rules, and other data necessary to detail the business rules provided by the ESM. The specification document can be used as a guidebook when integrating either COTS or GOTS software as components that back the ESM implementation.

6.4.2.   Engineering

6.4.2.1.   The contractor shall integrate ESM with additional NCES Core Enterprise Service including Security Services and Service Discovery. The integrations will need to follow an agile, iterative software development process and the contractor will be required to provide releases on a schedule defined by the government. The integrations will also be aligned with the ESM specification and architecture documents.

6.4.2.2.   The contractor shall develop testing documentation to include test cases and test scenarios in electronic and automated formats.   The contractor shall define all test related data sets and execute product-testing cycles prior to release approval. The contractor will perform regression testing as required and maintain metrics on test coverage.

6.4.2.3.   The contractor shall support the government in the definition of formal new release scope and the management of integration support requests. The contractor shall have formal participation at CCB meetings for review and approval of new release scope and integration support activities.

6.4.2.4.   The contractor shall produce key engineering documents and artifacts including the following:

- Integration guide

- Requirements documentation including use cases, Software Requirements Specification, and Requirements Traceability Matrix
- System architecture document
- Service specifications with annotated Web Services Description Language (WSDL) files
- User guides and tutorials
- Test plans, test scenarios and test suites
- Installation guides
- Developer/integrator guides

6.4.3. Outreach and Integration

6.4.3.1. The contractor shall provide hands-on support to the NCC Pilot program. The contractor will be required to support the portfolio members in architecting their solutions to integrate into the ESM architecture.

6.4.3.2. The contractor shall support program reviews and technical exchange meetings required by both the NCES program and community pilot programs (e.g. NCCP, Horizontal Fusion). The contractor will prepare briefings that communicate project status and technical details on the ESM. On the average, one technical exchange meeting or equivalent is expected per week with one deliverable (briefing, report, etc.) per meeting.

6.4.3.3. The contractor shall deliver scheduled knowledge transfer sessions to DISA personnel.

6.4.4. Technical Support

6.4.4.1. The contractor shall support the deployment and fielding of ESM to support pilot activities. The scope of the deployments will include instances of ESM in the following environments: DISA DECC (SIPRNET), COI, and NIPRNET. The contractor will provide hands-on support for installation, deployment, and other hosting-related issues for ESM Service.

6.4.4.2. The contractor shall support the capture of CDD-defined metrics to support test and evaluation.

6.4.4.3. The contractor shall support the development of C&A documentation and application level testing to support the deployment of ESM on NIPR/SIPRNET. The contractor will be required to support acceptance testing, vulnerability testing, etc. The contractor will also be required to develop key accreditation documentation artifacts including the SSAA and appendix T documents.

6.5. Task 5. Optional Horizontal Fusion Support

6.5.1. The contractor shall provide integration support for current release versions of the DISA NCES Service Discovery, Security Service, and ESM software.

6.5.2. The contractor shall provide help desk support for deployed versions of the DISA NCES software on a 24 by 7 basis and be responsible only for items considered defects in the currently deployed software.

6.5.3. The contractor shall provide help desk support to developers working with release versions of Service Discovery, Security Services, ESM or SDKs.

6.5.4. The contractor will include HF in all notifications of upcoming DISA NCES release content and provide technical exchange briefings on the Service Discovery, Security Services, and ESM as needed to facilitate integration into HF.

6.5.5. If an "HF specific" software patch is approved by DISA, the contractor shall supply requirements scope, level of effort and delivery schedule estimates for requested changes / enhancements. **Note:** HF requests must align with the NCES vision for the services roadmap.

7. Place of Performance

The activities shall be conducted primarily at contractor facilities, DISA locations, and DISA test facilities. It is expected that the contractor shall spend considerable time at the DISA location 5275 Leesburg Pike, Falls Church, Virginia, in meetings and discussing the schedules and other programmatic details with DISA program personnel. The contractor, with completed clearances, will be granted access to DISA facilities, as required. The Government will provide no permanent working space in any DISA facility.

The contractor shall be required to perform work associated with task orders in any of the 50 states. Approval of the TM is required before commencing any travel. Established Federal Government per diem rates will apply to contractor travel. Variations to authorized travel are acceptable only with the prior approval of the TM. Travel must be performed in accordance with the Joint Travel Regulation and its prevailing rates. Any travel required by the Contractor shall be reimbursable in accordance with the Federal Travel Regulations.

7.1. Anticipated Meeting Locations

The Contractor shall attend meetings at contractor facilities, at the government sites listed below, and at other locations, as mutually agreed and as needed. Potential government sites include, but are not limited to, the following:

DISA HQS, Arlington, VA

DISA location, Falls Church, VA

Pentagon, Arlington, VA

MITRE, McLean, VA

Lansdowne Conference Center, Lansdowne, VA

7.2. Anticipated Travel

At this time, the following annual travel is anticipated from Washington National Capital Region to the following destinations:

SPAWAR Charleston, SC

SPAWAR San Diego, CA

DECC Columbus, OH

8. Period of Performance

The anticipated period of performance for this order will be 306 days from date of award.

9. Deliverable Items / Delivery Schedule

9.1.   Deliverables. The Contractor shall deliver the items listed in the table below and in the quantity specified. CDRL/DIDs do not apply. Contractor shall furnish deliverables in contractor's format, subject to TM approval, unless otherwise specified in the statement of work. Deliverables <u>must</u> be developed in a format that is compatible with Microsoft Office 2000 applications.

9.2.   Standard Distribution. The contractor shall deliver one electronic copy of each deliverable and one paper copy, colored where necessary for understanding, to the TM. Electronic delivery shall be made via E-mail or CD unless other arrangements are made with the TM (such as posting to an FTP site, for example). A copy of cover letters transmitting final submissions of technical deliverables shall be sent to the Contracting Officer and the TM. Standard Distribution applies to all deliverables unless otherwise noted.

Task Number	Deliverables	Due Date
1.	**Task Order Management**	
	Management Plan	30 calendar days after date of award
	Monthly Status Reports	Tenth business day of the following month
	In-Progress Reviews (IPRs)	Quarterly
2.	**NCES Service Discovery**	
6.2.1.1	Architecture Document Service Discovery Specification Service Discovery WSDLs	90, & 210 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.2.1.2	Enterprise Deployment Document Deployment Strategy Document	90, & 210 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.2.1.3	Participation in working group meetings Meeting minutes and action lists	As required
6.2.1.4	Service Discovery Architecture CONOPS	90, 180 & 270 Calendar Days after Date of Award or

Task Number	Deliverables	Due Date
		as agreed to by Gov't and Contractor
6.2.2.1	Software Development Plan Service Discovery Reference Implementation	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.2.2.2	Web-based user interface software to support Service Publishing and Discovery lifecycle, including taxonomy and metadata management	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.2.2.3	Test Scenarios and test cases document. Automated SOAP Test scripts Summary execution reports Test Strategy document Release Test Plan document. Release test metrics	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.2.2.4	Stakeholder request list Level of Effort spreadsheets CCB Presentations	Last business day of each month
6.2.2.5	Integration guide Requirements documentation including use cases, Software Requirements Specification, and Requirements Tracability Matrix System architecture document Service specifications with annotated Web Services Description Language (WSDL) files User guides and tutorials Test plans, test scenarios and test suites Installation guides Developer/integrator guides Release Notes CONOPS Detail Design documents Unit test scripts	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor

Task Number	Deliverables	Due Date
	Source Code files Packaged Release Installer and Files	
6.2.2.6	SDK Development and Support	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.2.3.1	Log of all support activities assigned and completed Trip and site visit status reports	Last business day of each month for recurring or 5 business days after event
6.2.3.2	Project status and overview presentations	Quarterly
6.2.3.3	Training materials for Service Discovery Service	As required
6.2.4.1	Stakeholder request list Level of effort estimates Service Patch Schedule	Last day of each month
6.2.4.2	Load test Scripts Load test execution results summary	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.2.4.3	Metrics Report	As required
6.2.4.4	C&A documentation Appendix T documents Test execution summary reports	70, 140, 210 & 280 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
3.	**NCES Security Services**	
6.3.1.1	Security Services Architecture Document	90 & 210 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.3.1.2	Architecture Analysis and recommendation	90 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.3.1.3	Participation in working group meetings Meeting minutes and action lists	As required or 5 business days after event
6.3.1.4	Meeting minutes and action lists	5 business days after event
6.3.1.5	COTS Tools analysis document	60 Calendar Days after Date of Award or as agreed to by

Task Number	Deliverables	Due Date
		Gov't and Contractor
6.3.1.6	Security Services specification document	
6.3.2.1	Software Development Plan	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.3.2.2	Test Scenarios and test cases document. Automated SOAP Test scripts Summary execution reports Test Strategy document Release Test Plan document. Release test metrics	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.3.2.3	Stakeholder request list Level of Effort spreadsheets CCB Presentations	Last business day of each month.
6.3.2.4	Analysis and recommendation report	60 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.3.2.5	Integration guide Requirements documentation including use cases, SRS, and RTM System architecture document Service specifications with annotated Web Services Description Language (WSDL) files User guides and tutorials Test plans, test scenarios and test suites Installation guides Developer/integrator guides Release Notes CONOPS Detail Design documents Unit test scripts Source Code files	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor

Task Number	Deliverables	Due Date
	Packaged Release Installer and Files	
6.3.2.6	Detail Design documents Unit test scripts Source Code files Packaged Release Installer and Sample Application Files Release Notes	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.3.2.7	Detail Design documents Unit test scripts Source Code files Packaged Release Installer and Sample Application Files Release Notes	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.3.3.1	Log of all support activities assigned and completed Trip and site visit status reports	Last business day of each month for recurring or 5 business days after event
6.3.3.2	Technical presentations Status Presentations	As required
6.3.3.3	Knowledge-transfer briefings	As required
6.3.4.1	Stakeholder request list Level of effort estimates Service Patch Schedule	Last day of each month
6.3.4.2	Log of all support activities assigned and completed Trip and site visit status reports	Last business day of each month for recurring or 5 business days after event
6.3.4.3	Metrics Report	As needed by Gov't
6.3.4.4	C&A documentation Test execution summary reports Appendix T documentation	70, 140, 210 & 280 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
4.	**NCES Enterprise Service Management (ESM)**	
6.4.1.1	ESM Architecture Document	30 & 180 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.4.1.2	Deployment Architecture Analysis and recommendations / Options	60 & 180 Calendar Days after Date of Award or as

Task Number	Deliverables	Due Date
		agreed to by Gov't and Contractor
6.4.1.3	Participation in working group meetings Meeting minutes and action lists	As required
6.4.1.4	ESM specification document	90 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.4.2.1	Integration Development Plan	90 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.4.2.2	Test Scenarios and test cases document. Automated SOAP Test scripts Summary execution reports Test Strategy document Release Test Plan document. Release test metrics	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.4.2.3	Stakeholder request list Level of Effort spreadsheets CCB Presentations	Last business day of each month
6.4.2.4	Integration guide Requirements documentation including use cases, SRS, and RTM System architecture document Service specifications with annotated Web Services Description Language (WSDL) files User guides and tutorials Test plans, test scenarios and test suites Installation guides Developer/integrator guides Release Notes	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor
6.4.3.1	Log of all support activities assigned and completed Trip and site visit status reports	Last business day of each month for recurring or 5 business days after event

Task Number	Deliverables	Due Date
6.4.3.2	Technical presentations Status Presentations	As required
6.3.3.3	Knowledge-transfer briefings	As required
6.4.4.1	Stakeholder request list Level of effort estimates Service Patch Schedule	Last business day of each month
6.4.4.2	Metrics Report	As required
6.4.4.3	C&A documentation Test execution summary reports Appendix T documentation	90, 180 & 270 Calendar Days after Date of Award or as agreed to by Gov't and Contractor

10. Security

Contractor personnel must possess at least a current SECRET security clearance. The Contractor cannot claim lack of security clearance as justification for non-performance.

The Government will provide the Contractor unrestricted access to government facilities consistent with security clearances and policies. Access will only be granted during the period of performance specified above. Other designated personnel who have been granted the appropriate security clearance and escort privileges must continuously escort all contractor personnel not possessing the proper clearances who require entry to controlled areas.

The Contractor shall comply with local facility manager requirements for protection of government property while performing duties in government facilities.

In accordance with DISA Manpower, Personnel & Security Directorate (DISA/MPS - formerly ISBE) policy letter, subject Contractor Automated Data Processing Sensitivity Designations, dated 3 Jun 1996, the Contractor shall require ADP-II designation for access to the DISANet LAN. As required by DISA/MPS in the Industrial Security Program & DD Form 254 Contract Security Classification Specification Implementation Guide, dated 30 Sep 97, the following language is incorporated from Appendix E, Table 2:

"DoD 5200.2-R, DoD Personnel Security Program, requires DoD military and civilian personnel, as well as DoD consultant and contractor personnel, who perform work on sensitive automated information systems (ISs), to be assigned to positions which are designated at one of two sensitivity levels (ADP-I, ADP-II). These designations equate to Critical Sensitive, Non-critical Sensitive. The Contractor shall assure that individuals assigned to the following sensitive positions, as determined by the Government, have completed the appropriate forms.

DISA retains the right to request removal of contractor personnel, regardless of prior clearance or adjudication status, whose actions, while assigned to this task order, clearly conflict with the interests of the Government. The reason for removal will be fully documented in writing by the

Contracting Officer. When and if such removal occurs, the Contractor shall, within twenty (20) working days, assign qualified personnel to any vacancy(ies) thus created."

11. Government-Furnished Equipment /Government-Furnished Information (GFE/GFI)

No Government–Furnished Equipment is anticipated. GFI includes the NetOps Concept of Operations, as well as templates and other sample documents such as situation reports and trip reports. The contractor shall identify the need for additional GFI to the TM, by email. The TM will ensure the contractor has the necessary GFI.

12. Packaging, Packing and Shipping: As stated in the Schedule.

13. Inspection and Acceptance: As stated in the Schedule.

14. Other Pertinent Information or Special Considerations

14.1. Travel may be required to participate in site reviews or other meetings with customers. The Government must expressly approve travel outside the National Capital Region. Specific travel requirements will be coordinated with the Task Monitor and shall be in accordance with both Federal Acquisition Regulation (FAR) and Joint Travel Regulation (JTR) requirements and limitations. The Government anticipates some local travel may be required. Reimbursement for travel expenses will be made in accordance with the Federal Travel Regulations.

14.2. Other Direct Costs. Incidental supplies, equipment, and materials required for performance of this effort shall be identified in the contractor's proposal.

14.3. Section 508 Accessibility Standards.

Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended, is not applicable.